IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA	**)**	
	)	
v.	**)**	**Criminal No. 1:17CR34**
	)	**Hon. Liam O'Grady**
TAYLOR HUDDLESTON,	**)**	**Sentencing Date: February 23, 2018**
	)	
Defendant	**)**	

DEFENDANT TAYLOR HUDDLESTON'S
POSITION ON SENTENCING

On July 25, 2017, Defendant Taylor Huddleston entered a guilty plea to one count of Aiding and Abetting Computer Intrusions in violation of 18 U.S.C. § 1030(a)(5)(A). Mr. Huddleston understands that he committed a serious crime, and he is disgraced by and remorseful for his conduct. He looks forward to using his unique talents to benefit society after serving his sentence. Mr. Huddleston submits this memorandum to assist the Court in determining a sentence that is "sufficient, but not greater than necessary." 18 U.S.C. § 3553(a). After considering his background and offense conduct through the lens of the relevant statutory factors, Mr. Huddleston submits that the appropriate sentence is incarceration of no more than six (6) months followed by a significant period of supervised release conditioned upon six (6) months of home detention, community service, and forfeiture of assets.[1] These consequences, in addition to the consequences that accompany all felony convictions, are sufficient to punish Mr. Huddleston and deter unlawful conduct by others.

[1] The parties will be submitting a Consent Order of Forfeiture in the agreed-upon amount of $88,739.59.

OBJECTIONS TO THE PRESENTENCE REPORT

Mr. Huddleston has no objections to the Presentence Investigation Report ("PSR") filed on February 13, 2018. As explained below, however, Mr. Huddleston believes the Court should vary downward from a Guidelines sentencing range that unfairly inflates his culpability and that does not account for significant mitigating facts in this case.

BACKGROUND

I. Mr. Huddleston's History and Characteristics

Mr. Huddleston is a 27-year-old, self-made computer programmer living in Hot Springs, Arkansas. PSR at p. 2. He works as a carpenter and until last summer also was a freelance software programmer. *Id.* at ¶¶ 81-83. Mr. Huddleston is close with his mother, two brothers, and other family who live near him in Arkansas. *Id.* ¶ 72. Mr. Huddleston's mother raised him and his brothers on her own. *Id.* ¶ 73. He never knew his biological father. *Id.* ¶ 72. He spends his free time programming on the computer and playing videogames as well as enjoying low-tech hobbies like biking, woodworking, playing board games, and caring for a pet bird. *Id.* at p. 22. Before this case, Mr. Huddleston was never in trouble with the law. *Id.* ¶¶ 64-70.

Mr. Huddleston moved repeatedly throughout his childhood: from El Paso, Texas, where he was born, to various towns in New Mexico, and then to Arkansas as a teenager. *Id.* ¶¶ 72-74. Mr. Huddleston subsequently moved again within Arkansas. *Id.* ¶ 74. In all, Mr. Huddleston attended ***nine*** different schools throughout his childhood. *Id.* at p. 22. Mr. Huddleston's family had little money, and at times lived in mobile homes, trailers, and even outdoors in covered sheds. *See id.* ¶ 73; Exhibit 1 (Taylor Huddleston's Letter to the Court) at 1. This is a photograph of Mr. Huddleston's current home outside of Hot Springs:

This history and circumstances impeded Mr. Huddleston's scholastic and social development. He did poorly in school and found it difficult to make and keep friends. *Id.* ¶¶ 73, 79-80. Mr. Huddleston's highest level of formal education was completing the ninth grade, and after that, he attended high school only sporadically. *See id.* A recent psychological evaluation of Mr. Huddleston indicates that he has suffered throughout his life from Autism Spectrum Disorder and Social Anxiety Disorder.[2] Although these disadvantages do not excuse the serious crime to which he pled guilty, it has not been an easy life for Mr. Huddleston.

Mr. Huddleston started teaching himself computer programming in his late teens. Exhibit 3 at 2. In programming, Mr. Huddleston found something he loved and was talented at. He took refuge working on computers because it did not require uncomfortable, face-to-face interactions. *Id.* at 6. Mr. Huddleston worked countless hours over many years to learn to hone his craft, and eventually, found himself educating others on the internet about programming. Exhibit 2 (Letter from Jackie Schuhart). Mr. Huddleston hosted a YouTube channel where he shared tips and tricks with a dedicated following of a few hundred viewers.

[2] The psychological evaluation, attached as Exhibit 3, has been filed under seal because it contains private medical information.

Mr. Huddleston began selling software and freelance programming services with the goal of "mak[ing] enough money to lift [him]self out of poverty" and attaining a financially stable life. Exhibit 1 at 2. Unlike the two software programs at issue in this case, Mr. Huddleston's other programs were innocent and legal applications. Some recognized Mr. Huddleston's talent and asked him to do legitimate, "white hat security testing." *See* discovery production at US-00009642 (5/6/2014 email).[3]

Letters from family and friends, attached as Exhibit 2, confirm that Mr. Huddleston is a thoughtful, smart, and honest young man whose conduct in this case is not indicative of his true character. They emphasize Mr. Huddleston's dedication to helping others and "potential to . . . educate people with his computer knowledge." Exhibit 2 (Letter from Kathy Redd). These letters portray a young man who knows he did wrong but who genuinely cares for and wants to help others. Mr. Huddleston has great potential to make up for his past by using his skills to benefit society.

II. The Offense Conduct

In 2009, one of Mr. Huddleston's YouTube viewers told him that a "cracked" or free version of one of his programs, Net Seal, was being distributed on a website called Hackforums. Hackforums is an online forum where members discuss and trade hacking software and also converse about non-nefarious topics ranging from mobile applications to philosophy and politics. Mr. Huddleston was attracted to the website because of its active discussions on programming.

Mr. Huddleston marketed certain of his programs on Hackforums. He started marketing his program Net Seal in 2012. PSR ¶ 24. Net Seal is licensing software that allowed other

[3] The documents referenced herein from the discovery production are available to the Court upon request. Given the nature of the documents, counsel has chosen not to file them publicly.

programmers to protect their software. *Id.* ¶ 22. Net Seal on its own is not a malicious program; indeed its function was to simply allow sellers of software to make sure they received compensation for their work. *See id.* ¶¶ 22, 26, 31. Nor was Net Seal "advertised exclusively on Hackforums," as the government claims. Govt. Position on Sentencing at 2. Mr. Huddleston acknowledges, however, that Net Seal was used to sell malware. *Id.* ¶¶ 24-25. And, as is most relevant to this case, Net Seal was the program that Zachary Shames used to help protect and distribute his Limitless keylogger software. *Id.* ¶ 22. Mr. Huddleston acknowledges that by selling Net Seal on Hackforums—despite being "aware that the[] customers intended to use . . . the software for illegal and unauthorized computer intrusions"—he "acted with the purpose of furthering and aiding and abetting the[] illegal and unauthorized computer intrusions and causing them to occur." *Id.* ¶ 25.

By distributing Net Seal to Mr. Shames, for example, Mr. Huddleston "aided and abetted Shames's distribution of the Limitless keylogger to over 3,000 people who used it to infect . . . over 16,000 computers." *Id.* ¶ 32. Although he was not party to the conversations, Mr. Huddleston agrees the evidence shows that Mr. Shames discussed the capabilities of the Limitless keylogger with his customers who used the software. *See id.* ¶ 34. Mr. Huddleston sold Net Seal in October 2016 to a third party. *See* discovery production US-15264-65.

Another program Mr. Huddleston marketed on Hackforums was NanoCore. NanoCore is a "remote access tool . . . designed to allow a computer hacker to take complete control of a victim's computer for the purpose of performing" remote operations. *Id.* ¶ 36. NanoCore came with its own features and also utilized a plug-in system to allow third parties to add their own functionality. *Id.* ¶¶ 37-38. Mr. Huddleston marketed NanoCore on Hackforums from January 2014 through February 2016. *Id.* ¶¶ 35, 39. In doing so, Mr. Huddleston "caused [NanoCore] to

be distributed to over 350 people, some of whom [he] knew intended to use . . . [the] software for illegal and unauthorized computer intrusions." *Id.* ¶ 39. In February 2016, Mr. Huddleston sold NanoCore to a third party. *Id.* ¶ 35.

Mr. Huddleston agrees the evidence shows that an unidentified hacker used NanoCore "in or about August 2016"—six months after selling the program—to attempt a "spear phishing scheme" by sending the program via email to 6,000 targeted computers associated with vendors of an oil company. *Id.* ¶¶ 41-42. The unidentified hacker, from a "spoofed" email address that appeared to belong to the oil company, sent emails "stat[ing] that the victims owed money to [the oil company] and includ[ing] a PDF file attachment that purported to be an invoice" but "in fact contained a link to a malicious executable" version of NanoCore. *Id.* ¶ 42. The oil company itself did not suffer any financial or data loss from the attack, *see* discovery production US-00000001-0002, and the government has not introduced substantive evidence of financial or data loss that the vendors suffered. The PSR says that "[d]ue to the number of victims and/or the complexity of restitution issues, the determination of specific restitution amounts to any individual victim is unavailable at this time." *Id.* ¶ 47. The government estimates that a "majority of the identified victims thus far are foreign individuals residing in Asia and Africa." *Id.*

Mr. Huddleston understands and accepts that he broke the law by marketing Net Seal and NanoCore on a website frequented by users who would likely use the programs for malicious purposes. As he writes in his letter to the Court, "[i]ts important to me that you know how sincerely remorseful I am about the circumstances I've put others and myself into. It haunts me knowing that innocent people were and likely still are being victimized because of my actions." Exhibit 1 at 1. Mr. Huddleston knows that he has no one to blame but himself, and is prepared to

serve the sentence this Court finds appropriate. His actions before and after his arrest illustrate his sincere remorse and dedication to using his talents to benefit society and make amends for his illegal conduct.

III. Mitigation Before Pleading Guilty

Mr. Huddleston has admitted his guilt and accepts responsibility for his illegal actions. It bears noting, however, that documents produced by the Government demonstrate that Mr. Huddleston tried, with unknown success, to mitigate malicious use of NanoCore and Net Seal even before being arrested and pleading guilty.

Mr. Huddleston discouraged or threatened some users whom he suspected used the programs maliciously. For example, in November 2014, Mr. Huddleston asked a NanoCore user to confirm that "the computer in question is a machine you own[,] correct, or at least have permission to install NanoCore on, correct? If not, it would be a breash (sic) of the terms of service and probably your local laws." Discovery production US-00010671 (11/27/2014 email). Mr. Huddleston advised other users that he had a "zero tolerance policy" for anyone using the programs for "malicious activities." *Id*. at US-00011079 (1/21/2015 email). When one user inquired whether NanoCore could be detected by antivirus software, Mr. Huddleston responded that he "ha[s] no intention of ever trying to hide NanoCore from anti-virus software." *Id*. at US-00011645-1646 (3/5/2015 email). He told another user that "NanoCore is not [undetectable to antivirus] nor will I ever attempt to hide it from anti-virus software." *Id.* at US-00011659 (3/6/2015 email). Hackforums posts confirm that Mr. Huddleston faced criticism after he banned users for using his programs maliciously. *See, e.g.*, *id.* at US-00016088 ("Also nanocore wouldnt be as bad if they were not hypocrypts (sic) and banned people for spreading but yet sell on a 'hack' forum."). Disgruntled users retaliated by using so-called "chargeback" schemes that

allowed them to effectively steal money from Mr. Huddleston's PayPal accounts. *See id.* at US-00016148 (10/12/2016 online forum post).

Over time, in response to malicious use, Mr. Huddleston stripped his software of certain features. By 2015, for example, Mr. Huddleston had removed NanoCore's keylogger function. *See id.* at US-00016065 (8/16/2015 online forum post noting program's lack of "official keylogger / password recovery"). He also removed a password recovery function. *See id.* Another of Mr. Huddleston's pre-arrest attempts to mitigate NanoCore-related fallout was anonymously sharing the program's source code with a security researcher in early 2016. Mr. Huddleston hoped the prominent security researcher would publish vulnerabilities in NanoCore's code and thereby discourage or undermine continued, unlawful use of the program. The researcher did in fact post details about NanoCore's code and vulnerabilities on Twitter and his blog.[4]

More broadly, the evidence in Mr. Huddleston's case demonstrates that, by 2015 and 2016, he became increasingly uneasy about selling software that he knew was being used maliciously. Knowing that people were using his software maliciously "made [Mr. Huddleston] sick and ashamed" and "depressed and empty." Exhibit 1 at 2. Mr. Huddleston began more harshly admonishing suspected malicious users and planned a way out of the business he created. *Id*. Mr. Huddleston eventually sold the two at-issue programs to third parties because "no amount of money was worth" the ill feeling mounting in Mr. Huddleston. By 2016, about a month before government agents came to his home, Mr. Huddleston had announced publicly his

[4] *See* LINKCABIN, *NanoCore Cracked Alcatraz-Leaving The Door Open*, Blog (Mar. 25, 2017), https://itsjack.cc/blog/2017/03/nanocore-cracked-alcatraz-leaving-the-door-open/; linkcabin (@LinkCabin), Twitter (Mar. 25, 2017, 3:45 AM), https://twitter.com/LinkCabin/status/845587501288972292.

interest in creating a program "that would contain useful functions for *combating* malicious actors." *See id.* at US-00016150 (10/23/2016 online forum post) (emphasis added).

Mr. Huddleston is not minimizing his offense conduct. He accepts responsibility for creating and selling Net Seal and NanoCore to users who likely would use the programs maliciously, and he acknowledges the existence of documents and other communications showing that he was aware of and, by selling his programs, aided illegal activity. In his letter to the Court, Mr. Huddleston writes that he "could have been a powerful force for good and . . . squandered the opportunity." Exhibit 1 at 2-3. But just as the evidence supported Mr. Huddleston's liability for aiding and abetting computer intrusions, it also shows that, even before he was arrested, Mr. Huddleston tried to discourage and limit malicious use of the programs that he marketed.

IV. Mitigation Since Pleading Guilty

As part of his Plea Agreement, Mr. Huddleston agreed to cooperate and provide whatever assistance is necessary to aid the government in the investigation or prosecution of others, especially third-party hackers who have or are using malware against innocent victims. The nature of that cooperation should remain confidential, but suffice it to say that Mr. Huddleston has personally met with government agents, spoken with them over the telephone, and provided information that he believed would be helpful in the government's investigations. And although it is unknown whether his cooperation will prove "substantial" enough to merit a motion for reduction of sentence, Mr. Huddleston has done and will continue to do everything he can to help the government find and prosecute malicious actors on the internet.

SENTENCING ARGUMENT

Mr. Huddleston made a serious and consequential decision by using his self-taught programming skills to create software that he knew malicious third-party hackers used to commit

computer intrusions. That decision is why he pled guilty and will be sentenced by this Court. A close look at Mr. Huddleston's personal background and offense conduct, however, makes clear that a significant downward variance from the U.S. Sentencing Guidelines is appropriate in his case. He has accepted responsibility, expressed genuine remorse, cooperated with law enforcement, and shown willingness and ability to help defend against malicious attacks that are becoming increasingly common in this country. Mr. Huddleston poses little risk of reoffending, and to the contrary, is uniquely positioned to benefit society as an expert programmer and fundamentally good person. Treatment of Mr. Huddleston's mental health conditions—which could explain his once-outsized reliance on internet communications—make him even less likely to run afoul of the law again. For these reasons, Mr. Huddleston respectfully requests that the Court impose a below-Guidelines sentence of no more than six (6) months of imprisonment followed by a significant period of supervised release conditioned upon six (6) months of home detention, community service, and forfeiture of assets.

I. A Significant Downward Variance from the Guidelines Range Is Warranted.

The Guidelines are advisory. *United States v. Booker*, 543 U.S. 220, 226 (2005). Imposing a sentence is not a mathematical exercise. District courts make "an individualized assessment based on the facts presented" after calculating the advisory Guidelines range. *Gall v. United States*, 552 U.S. 38, 50 (2007); *see United States v. Hughes*, 401 F.3d 540, 546 (4th Cir. 2005). The Guidelines range is but one of several factors a court must consider when imposing a sentence, and it is legal error to "presume that the appropriate sentence . . . will come from the Guidelines." *United States v. Mendoza-Mendoza*, 597 F.3d 212, 216-17 (4th Cir. 2010); *see also Nelson v. United States*, 555 U.S. 350, 352 (2009) (per curiam); *Spears v. United States*, 555 U.S. 261, 263-64 (2009).

Mr. Huddleston requests a substantial downward variance from his Guidelines sentencing range because: (1) the astounding 16-level fraud loss enhancement unfairly exaggerates Mr. Huddleston's culpability, and (2) more generally, the § 3553(a) sentencing factors weigh in favor of a below-Guidelines sentence. The sentence Mr. Huddleston proposes—no more than six months of incarceration followed by a significant period of supervised release conditioned upon six months of home detention, community service, and forfeiture of assets—takes into account the seriousness of Mr. Huddleston's offense, as well as his age and health, lack of criminal history, cooperation and acceptance of responsibility, and the severe collateral consequences that will come with his conviction. It is a punishment that, while significant, "fit[s] the offender and not merely the crime." *Pepper v. United States*, 562 U.S. 476, 487-88 (2011).

II. The 16-Level Loss Enhancement Unfairly Exaggerates Mr. Huddleston's Culpability And Inflates His Guidelines Range.

For purposes of calculating the Guidelines range, Mr. Huddleston agrees that a 16-level loss enhancement applies to his case. However, considering the § 3553(a) factors, that enhancement is unfair and overstated, and should not drive the Court's ultimate conclusion on his sentence.

First, the 16-level increase is disproportionate to Mr. Huddleston's offense. It is nearly triple Mr. Huddleston's base offense level of 6. There are no other double-digit specific offense enhancements anywhere in Sections 2A or 2B of the Guidelines ("Offenses Against the Person" and "Basic Economic Offenses," respectively). The 16-level enhancement for loss assessed against Mr. Huddleston is *as large as any other enhancement in the Guidelines*.[5]

[5] Besides loss amount in a § 2B1.1 case, the largest specific offense enhancements appear to be: Willfully boarding an aircraft with a dangerous weapon or material without regard for the safety of human life (Section 2K1.5(b)(1), 15 levels); trafficking, receiving, or possessing

By fueling a Total Offense Level of 27, the fraud Guideline assigns a sentencing range *higher than* that which applies to offenses that create significantly more dangers to society, including *violent* offenses like:

- bombing of an airport, aircraft or mass transit facility (Section 2K1.4(a)(1), base offense level 24);
- bank robbery under threat of death with bodily injury (Section 2B3.1, base offense level 20 + 6 levels for bank, threat, and injury);
- distribution of child pornography for pecuniary gain (Section 2G2.2(a)(1), base offense level 18 + 5 levels for the financial gain);
- trafficking of up to 3.5 kilograms of cocaine (Section 2D1.1(c)(7), base offense level 26); and
- aggravated armed assault with a discharged firearm resulting in serious life-threatening bodily injuries (Section 2A2.2, base offense level 14 + 10 levels for the discharge of the firearm and the injuries).

It is unreasonable to assign a comparable offense level for defendants who commit violent crimes, such as the ones listed above, and Mr. Huddleston, who committed a non-violent offense where there is no documented financial loss to any victim. *See United States v. Corry*, 206 F.3d 748, 751 (7th Cir. 2000) ("That the loss overstates the seriousness of the offense is . . . an encouraged basis for departure."); *United States v. Adelson*, 441 F. Supp. 2d 506, 509 (S.D.N.Y. 2006) (noting the "inordinate emphasis that the Sentencing Guidelines place in fraud cases on the amount of actual or intended financial loss . . . without, however, explaining why it is appropriate to accord such huge weight to such factors"). Comparing sentencing enhancements is an imperfect but instructive exercise. And it simply cannot be the case that, in almost all federal criminal law, the most serious aggravating factor is the amount of loss in an economic crime case.

---

a portable rocket, missile, or launcher (Section 2K2.1(b)(3)(A), 15 levels); and bid-rigging or price-fixing, if the volume of commerce exceeds $1,850,000,000 (Section 2R1.1(b)(2)(H), 16 levels).

The "mechanical correlation between loss and offense level" is "[o]ne of the primary limitations of the guidelines, particularly in white-collar cases . . . ." *United States* v. *Ranum*, 353 F. Supp. 2d 984, 990 (E.D. Wis. 2005). The Guidelines do not take into account a host of other relevant factors, including what motivates a person to commit a crime: "[f]or example, the guidelines treat a person who steals $100,000 to finance a lavish lifestyle the same as someone who steals the same amount to pay for an operation for a sick child." *Id.* This is the fundamental flaw in relying so heavily on a single criterion – loss amount – to drive sentences, and is more reason to give the Guidelines less weight when fashioning a sentence here.

Second, the 16-level loss enhancement is too speculative and attenuated to support such a drastic increase in Mr. Huddleston's sentence. The logic underlying the 16-level loss increase is simple: (1) third-party hackers used NanoCore and/or the Limitless keylogger to attempt to infect 16,847 computers; (2) the Government determined, based on an FBI survey of four malware remediation companies, that "the reasonable costs to repair a computer damaged by the malware is $200"; (3) the loss amount is 16,847 computers multiplied by $200 per computer, or $3,369,400. PSR ¶ 45. This number, however, is a fiction. $3,369,400 has nothing to do with *actual* expenditures by companies or individuals to respond to hacking attempts, and it does not reflect "specific restitution amounts to any individual victim." *Id*. ¶ 47. The PSR acknowledges that "determination[s] of specific restitution amounts to any individual victim [are] unavailable at this time." *Id*. ¶ 47.

Further, the reference to an FBI survey of four private companies raises more questions than it answers. *Id*. ¶ 45. The PSR does not explain whether the survey concerned Mr. Huddleston's programs specifically or malware generally. The estimates do not reflect any facts about the supposed targets of the third-party hacking attempts that would allow a

particularized conclusion about loss that Mr. Huddleston's programs caused. Large sophisticated targets likely respond and spend differently in response to hacking attempts than small unsophisticated targets – but the PSR is silent on who suffered loss.

For example, the government references a "phishing scheme" email from an unknown hacker (not Mr. Huddleston), attaching Mr. Huddleston's program NanoCore, to various commercial recipients – and ignores the possibility that email recipients thwarted the attack and avoided loss by not opening the email or clicking the link to download NanoCore. PSR ¶ 42; Govt. Position on Sentencing at 4. As noted previously, moreover, the targeted oil company did not suffer any actual financial loss from the scheme. S*ee* discovery production US-00000001-0002.

To bolster the reasonableness of its loss calculations, the government has cited a January 5, 2018 letter from Bill Wright, Director of Government Affairs at the antivirus firm Symantec. The letter says "Symantec received notifications of [NanoCore] detections from 107,813 unique devices globally" between December 14, 2014 and December 13, 2017. That statistic may seem shocking at first blush but, as explained in a declaration, attached as Exhibit 4, from cybersecurity expert James O'Gorman, there are myriad reasons that the purported "detections" would not result in damage or may not even indicate the presence of NanoCore. In sum, the letter from Mr. Wright "is of limited utility." Exhibit 4 (O'Gorman Declaration).

Although Mr. Huddleston agrees that a 16-level loss enhancement applies as a matter of Guidelines interpretation, he disagrees that considering the § 3553(a) factors, such a dramatic increase in his offense level should be used to justify a sentence that would be based on a factual basis and methodology that is at best attenuated to this case and at worst speculative. Courts routinely decline to increase sentences based on loss amounts that are unknown at the time of

sentencing or "too attenuated and too speculative to support a criminal sentence." *United States v. Galvez*, 108 F. Supp. 2d 1369, 1373 (S.D. Fla. 2000); *see United States v. Butler*, 578 F. App'x 178, 181 (4th Cir. 2014) ("[w]hen calculating a loss amount for purposes of a sentencing enhancement, a district court is required to make a 'reasonable estimate' of the loss amount sustained by the fraud victim"); *United States v. Brooks*, 111 F.3d 365, 373-74 (4th Cir. 1997) (affirming district's court conclusion that "the government's method of proving loss in this case was simply too speculative"). That should be the case here.

Third, a below-Guidelines sentence is justified because of the enormous disparity between the Guidelines loss amount ($3,369,400) and the amount Mr. Huddleston gained from his offense. The Consent Order of Forfeiture that the parties signed recognizes that "the proceeds that the defendant obtained, directly or indirectly" from the offense conduct amount to a total of $88,739.59. The government may argue that he actually received more, but, regardless, it is beyond dispute that Mr. Huddleston gained far less from his conduct than was purportedly lost. Selling software allowed Mr. Huddleston to be financially independent despite his stilted start in life, but he never lived an opulent lifestyle. He lives in a modest home in a rural area. Mr. Huddleston works as a carpenter's assistant installing cabinets. He does not own a car or drive. Mr. Huddleston's liabilities outweigh his assets and he is financially unable to pay a fine. PSR ¶ 85. The imbalance between Mr. Huddleston's limited financial gain and the millions of dollars in "loss" is more reason to vary downward from a Guidelines range that is unfair in light of Mr. Huddleston's specific circumstances. *See* Sentencing Commission Pub. Hr'g, Comments of Preet Bharara at 45-46 (Feb. 16, 2011);[6] David Debold & Matthew Benjamin, Essay, "*Losing*

[6] Available at http://www.ussc.gov/policymaking/meetings-hearings/february-16-2011 (last visited Feb. 12, 2018).

Ground" – In Search of a Remedy for the Overemphasis on Loss and Other Culpability Factors in the Sentencing Guidelines for Fraud and Theft, 160 U. Pa. L. Rev. PENNumbra 141, 155 (2011) (noting that "the amount of the defendant's pecuniary gain should be a more consequential sentencing input" than intended loss).

III. Relevant Statutory Factors Support Mr. Huddleston's Request For A Downward Variance.

In sentencing Mr. Huddleston, the Court will consider statutory factors including (1) the nature and circumstances of the offense; (2) the history and characteristics of the defendant; (3) the kinds of sentences available; (4) the Guidelines range; (5) the need to avoid unwarranted sentencing disparities; (6) the need for restitution; and (7) the need for the sentence to reflect the seriousness of the offense, promote respect for the law, provide just punishment for the offense, afford adequate deterrence, and provide the defendant with needed educational or vocational training, medical care, or other correctional treatment. *See* 18 U.S.C. § 3553(a). A district court must weigh each factor and impose a sentence that constitutes the least amount of imprisonment necessary to achieve the statute's goals.

Applying those factors and principals to Mr. Huddleston's case shows the fairness of Mr. Huddleston's proposed, below-Guidelines sentence. The nature and circumstances of Mr. Huddleston's offense are admittedly serious. Mr. Huddleston committed a felony by aiding and abetting computer intrusions and he has sincere remorse for doing so.

That said, Mr. Huddleston's sentence should reflect that he was not personally involved in any hacking. He did not intrude into any computer to steal information, spy, or "empty a victim's bank account." Govt. Position on Sentencing at 11. It should matter that Mr. Huddleston is not himself a hacker. It should also matter that other than by selling his software, Mr. Huddleston did not financially profit from any hacking conducted by third parties.

The Court can consider Mr. Huddleston's repeated attempts to mitigate damage resulting from his programs, both before and after he was arrested. These attempts admittedly were insufficient to stop the distribution of the programs for which Mr. Huddleston pleaded guilty, but they help paint a fuller picture of Mr. Huddleston's culpability. Finally, no victims have come forward to claim that Mr. Huddleston's offense caused physical or financial damage. The same cannot be said for defendants who personally participated in hacking attacks that caused real damage to real victims, including by stealing their private information. For these reasons, the government's citation to its own sentencing memorandum in *United States v. Rappa*, 14-CR-544 (S.D.N.Y.) – a case where "an individual . . . activate[d] the web cameras of several victims and capture[d] images of them engaging in sexual activity in their bedrooms" – is irrelevant here and is an inapt comparison to Mr. Huddleston's offense conduct. *See* Govt. Position on Sentencing at 12.

Mr. Huddleston's history and characteristics counsel toward a below-Guidelines sentence. Mr. Huddleston's youth did not set him up for traditional success as most would understand it. He moved repeatedly, struggled to make friends, and did not complete high school. Programming was an escape that Mr. Huddleston took too far, and he regrets falling into behavior that he admits was criminal. A recent psychological evaluation of Mr. Huddleston revealed for the first time that he has suffered throughout his life from Autism Spectrum and Social Anxiety Disorders. This discovery helps explain why Mr. Huddleston engrossed himself in online relationships that caused less anxiety and embarrassment than in-person conversations. It is too late to speculate whether proper treatment would have helped Mr. Huddleston avoid committing the criminal offense to which he pleaded guilty, but understanding and treating the disorders going forward make him less likely to reoffend.

Despite problems at school and with real-world relationships, Mr. Huddleston achieved a level of programming expertise that required ingenuity and hard work. Letters submitted on Mr. Huddleston's behalf, attached as Exhibit 2, attest that he is not only smart and hardworking but also caring. He is "always there to lend a hand." Exhibit 2 (Letter from Kathy Redd). The letters speak to Mr. Huddleston's "potential to help educate people with his computer knowledge." *Id*. Indeed, the 250-or-so pages of Mr. Huddleston's online forum posts produced in this case are replete with instances in which he offers free (and often unsolicited) advice to other programmers. While Mr. Huddleston should have been more cautious about sharing advice with bad actors, his online posts show his unmistakably selfless and helpful nature. This case was "shocking" for loved ones who came to know Mr. Huddleston as a person outside the two programs for which he is being sentenced.

Further, a below-Guidelines sentence for Mr. Huddleston would fulfill "the need to avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct." 18 U.S.C. § 3553(a)(6). On January 26, 2018, the Court sentenced Mr. Shames – at one point an alleged coconspirator of Mr. Huddleston's – to, *inter alia*, 6 months of incarceration, to be followed by 2 years of supervised release conditioned upon 6 months of home confinement. *United States v. Shames*, 1:16-CR-289, ECF 41. There are of course differences between the cases and men being sentenced. But their offense conduct and the programs they sold are strikingly similar. As the Court knows, to collect payments for his product Limitless keylogger, Mr. Shames used Mr. Huddleston's program Net Seal. Their offenses are necessarily intertwined. Mr. Huddleston's other program, NanoCore, had some of the same functionalities as Limitless. Mr. Shames and Mr. Huddleston were both minors when

they started programming generally. Given the substantial similarities, Mr. Huddleston's sentence should bear some relation to that received by Mr. Shames.

Mr. Huddleston's sentence likewise should resemble those from *United States v. Dennis Collins, et. al.*, 1:13-cr-00383-LO, another case in this Court. The twelve defendants in *Collins* were originally charged with felony conspiracy for "participat[ing] in a worldwide conspiracy as part of the online group Anonymous in a campaign . . . to engage in a coordinated series of illegal cyber-attacks against victims." *See, e.g., id.* ECF 431 (Heller Statement of Facts). Ultimately, the defendants pled guilty to a misdemeanor offense, and despite having directly participated in identifiable computer intrusions and causing losses exceeding $8.9 million, the *Collins* defendants were sentenced only to time-served, which amounted to short periods of incarceration (e.g., 30 days or less). Mr. Huddleston did not directly participate in identifiable computer intrusions and his sentence – and its relation to the *Collins* sentences – should reflect that. For the same reasons, Mr. Huddleston believes that the sentence in *United States v. Michael Hogue*, 1:13-cr-12 (S.D.N.Y.), is instructive here. The defendant in *Hogue* pleaded guilty to distributing malware and personally "us[ing] malware to infect computers." *Id.* ECF 36 at 1; ECF 36. On January 29, 2016, the *Hogue* defendant was sentenced in the Southern District of New York to five years of probation and 500 hours of community service. *Id.* Mr. Huddleston's offense conduct and circumstances compel a similar, below-Guidelines sentence.

Mr. Huddleston's sentence should reflect the seriousness of the offense, promote respect for the law, provide just punishment for the offense, afford adequate deterrence, and provide the defendant with needed educational or vocational training, medical care, or other correctional treatment. Mr. Huddleston has respect for the seriousness of his offense and for the law. His

enthusiastic cooperation with the government since pleading guilty confirms that Mr. Huddleston's remorse and resolve to do good are authentic. Neither Mr. Huddleston's offense nor his background suggests that the Court need impose a harsh sentence to adequately deter him from further violations. Mr. Huddleston will face lifelong consequences from his pleading guilty to a felony, and that is deterrence enough. The government's argument that the sentence should "deter other malware developers" who "are at the heart of the problem" is not supported by any authority besides a citation to a case about a former healthcare executive whose securities fraud caused more than $1 billion in losses. *See* Govt. Position on Sentencing at 13 (citing *United States v. Martin*, 455 F.3d 1227, 1240 (11th Cir. 2006)). Mr. Huddleston disagrees that he should receive a more severe penalty to deter unidentified third-party hackers based on the government's subjective view of what motivates their behavior.

A minimal period of incarceration with home detention (so that he can maintain his employment) are most appropriate given the treatment required by Mr. Huddleston's recent diagnoses of Autism Spectrum Disorder, Social Anxiety Disorder, and moderate Alcohol Use Disorder. As to the latter, Mr. Huddleston requests that if the Court orders incarceration, it also recommend that he be considered for the Residential Drug Abuse Program (RDAP).

In sum, the relevant statutory factors warrant a substantial downward variance from the Guidelines range. Evaluating Mr. Huddleston's offense conduct and circumstances through the lens of the sentencing factors renders a much more reliable conclusion about his culpability than does the inflated, attenuated, and assumptions-heavy Guidelines calculation.

CONCLUSION

Mr. Huddleston respectfully requests that the Court impose a sentence not to exceed 6 months of imprisonment with a significant period of supervised release conditioned upon no more than 6 months of home detention, community service, and forfeiture of assets. Mr. Huddleston also recommends that the Court not impose a fine given his inability to pay one. PSR ¶ 85. If the Court orders prison time, Mr. Huddleston asks that he be designated to FCI Texarkana, a low-security facility in Texarkana, TX, and that he be recommended for RDAP. He also requests that he be permitted to self-surrender given his compliance with his terms of release. *See id*. ¶ 8 (Mr. Huddleston "has been compliant with all aspects of his bond").

Respectfully submitted,

TAYLOR HUDDLESTON
By Counsel

/s/

Kenneth P. Troccoli
Virginia Bar Number 27177
Attorney for the defendant
Assistant Federal Public Defender
1650 King Street, Suite 500
Alexandria, Virginia 22314
(703) 600-0870 (T)
(703) 600-0880 (F)
Kenneth_Troccoli@fd.org

Hayter L. Whitman
Admitted Pro Hac Vice
Pro Bono Co-Counsel for the defendant
Wilkinson Walsh & Eskovitz LLP
2001 M Street, NW, 10th Floor
Washington, DC 20036
(202) 847-4001 (T)
(202) 847-4005 (F)
hwhitman@wilkinsonwalsh.com

CERTIFICATE OF SERVICE

I hereby certify that on February 16, 2018, I will electronically file the foregoing pleading with the Clerk of the Court using the CM/ECF system, which will then send a notification of such filing (NEF) to the following:

Kellen Dwyer, Esq.
Office of the U.S. Attorney
2100 Jamieson Avenue
Alexandria, Virginia 22314
(703) 299-3700
Kellen.Dwyer@usdoj.gov

Pursuant to the Electronic Case Filing Policies and Procedures, a courtesy copy of the foregoing pleading will be delivered to Chambers within one business day of the electronic filing, and to United States Probation Officer Jennifer Lyerly.

/s/

Kenneth P. Troccoli
Virginia Bar Number 27177
Attorney for the defendant
Assistant Federal Public Defender
1650 King Street, Suite 500
Alexandria, Virginia 22314
(703) 600-0870 (T)
(703) 600-0880 (F)
Kenneth_Troccoli@fd.org (email)